



Privacy Impact Assessment for Ginnie Mae Contractors

[Ginnie Mae](#) (GNMA-RFS)

Information Management Division

October 26, 2010

Version 1.5

Introduction

The purpose of this Privacy Impact Assessment is to help the Information Management Division (IMD) identify Ginnie Mae's information systems that process, store, use, and distribute data covered under the Privacy Act of 1974.

Ginnie Mae is responsible for ensuring the privacy and confidentiality of Personally Identifiable Information (PII) it collects, maintains, or disseminates from or about members of the public. Personally Identifiable Information includes information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.)

Instructions:

1. Fill out Part 1 of this study.

You may fill out the study electronically, but you must print it out to sign and mail it.

2. If you check yes to any of the questions about PII data in Section c of Part 1, you must also fill out Part 2.

Please be as descriptive as possible in answering the questions. You may use additional paper if necessary.

3. Sign and date the form, and then mail it to the following address via a secure mail service:

Ginnie Mae
Attention: Chitranjan Khandpur
451 7th Street SW
Room # B-133
Washington, DC 20410

If your organization processes, stores, uses, or distributes PII data, a security analyst working with the Ginnie Mae Information Management Division (IMD) will contact you to arrange a brief interview regarding how the PII data is being protected from unauthorized use, disclosure, or loss. These interviews usually last less than an hour, and you are not required to travel (the security team will come to your site).

Thank you for helping protect Ginnie Mae PII/privacy data.

Part 1: Privacy Data Determination

Please review Section A and fill out Sections B and C of Part 1.

A. System Information

If any information is incorrect in this section, please strike through it, correct it, and then initial the correction.

| System Information | |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System Name | GNMA Reporting and Feedback System (RFS) |
| System Description | The Reporting and Feedback System (RFS) is designed to replace legacy systems including the Ginnie Mae Portfolio Analysis Data System (GPADS), Mortgage Based Securities Information System (MBSIS) and several components of Web Services. RFS inherits and enhances the existing functionalities of the above legacy systems, eliminates old business processes and provides the newly added reporting and feedback functionality delineated in Ginnie Mae's Business Process Improvement (BPI) recommendations. |
| Name of System Provider | Deloitte & Touche LLP |
| Ginnie Mae Information Owner | Cheryl Owens |

B. System Provider Contact Information

Please enter the names and contact information for those personnel with primary responsibility for the Ginnie Mae information system.

| Contact Name | Title | Phone | Email |
|---------------------|----------------------|--------------|-----------------------------|
| Richard Parker | Development Manager | 301-721-5906 | richard.t.parker@lmco.com |
| Deborah Holmes, CIO | Authorizing Official | 202-708-1535 | deborah.v.holmes@hud.gov |
| Chitranjan Khandpur | RFS System Owner | 202-475-6555 | Chitranjan.Khandpur@hud.gov |
| | | | |
| | | | |
| | | | |

C. PII Data Processed by System

What Personally Identifiable Information (PII) is collected or stored on your Ginnie Mae information system(s)? Please check yes or no in the box provided.

| Type of PII Data | Yes | No |
|---------------------------------------------------------------------------------|-------------------------------------|-------------------------------------|
| 1. Name | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 2. Social Security Number (SSN) | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 3. Home address | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 4. Home telephone | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 5. Personal email address | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 6. Date of birth | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 7. Driver's license/state ID number | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 8. Race (e.g., Caucasian, African-American, American Indian, etc.) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 9. Religion | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 10. Ethnicity/national origin (e.g., Canadian, South African, etc.) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 11. Biometric information (e.g., fingerprint, voiceprint, photograph, etc.) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 12. Financial information (loan number, credit score, credit card number, etc.) | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 13. Passport number | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 14. Permanent and Alien registration number (Green Card) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 15. Insurance policy number | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 16. Digital/electronic signature information | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 17. Medical/psychological information | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 18. Criminal history | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 19. Mother's maiden name | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 20. Drug test results | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 21. Marital status | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 22. Education history | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 23. Gender/sex | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 24. Income data | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 25. Employment history | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 25. Tax Identification Number, Employee Identification Number | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 26. Other (please specify): | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Part 2: Privacy Data Details

If you answered yes to any question in Part 1, Section c of this form, please answer the questions below as completely as possible.

| | |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Does your Ginnie Mae system process, store, or collect PII data about more than 10 individuals? |
| | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No RFS processes, stores and collects personally identifiable information for portfolio and risk analysis. A large sampling base is required for data mining activities and portfolio analysis. |
| 2. | On what type of media is the PII data stored or collected? (For example, is the information collected via the Web, email, CDs, paper forms, etc.?) |
| | PII is collected monthly via EDI 203 transaction set over an ISDN connection. PII is then stored in an Oracle database in RFS. |
| 3. | What are the sources of the PII data? From whom is the information collected (e.g., government employees, contractors, consultants, the public)? |
| | RFS collects PII data from Issuers, Service Bureaus and Federal Agencies (name, SSN, address, and financial information (such as loan numbers) for validation, matching, queries, and reporting. These instances of collection are necessary to conduct the business purpose RFS is intended to serve. The collection and transfer of any and all PII has been minimized to the extent possible to lessen any associated risk. PII is initially collected by issuers from loan borrowers. Issuers then upload loan borrowers PII with other monthly loan data to RFS. |
| 4. | Why is the PII data stored or collected? What is the functionality of the system and the purpose that the records and/or system serve? |
| | RFS processes, stores and collects personally identifiable information for portfolio and risk analysis, to determine SCRA reimbursement eligibility and to process SCRA reimbursement requests. RFS provides Ginnie Mae management, Account Executives and analysts with access to loan level data and pool level data, pool accounting data, external agency and related data for use in issuer and securities monitoring, policy enforcement, and analysis as needed. Issuers, trading partners, and other authorized parties also have access, depending on security profiles, to RFS loan and pool level data as approved by Ginnie Mae. RFS also uses the collected PII data to verify against existing records. |
| 5. | How is information transmitted to and from the system? |
| | The RFS system protects the confidentiality of the transmitted information through VPN and soft token during authentication. All communication lines between NaviSite, Deloitte, LMIT and BNY will be configured to use AES256 bit encryption in compliance with FIPS 140-2 |

| | |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | guidelines. |
| 6. | What are the interconnections with other systems. |
| | <p>RFS connects with GMEP GSS/EWODS. GMEP/EWODS is a relational database that will store transaction processing data. This repository will store data from all of Ginnie Mae's Enterprise applications including RFS. Both GMEP/EWODS and RFS are owned by the same system owner. Hence an Information Sharing Agreement is not required at this time.</p> <p>Annually, the interconnections will be reviewed for continued validity and required access.</p> |
| 7. | What is the current / intended use of the PII data? What is the functionality of the system and the purpose that the records and/or system serve? |
| | <p>RFS processes, stores and collects personally identifiable information for portfolio and risk analysis, to determine SCRA reimbursement eligibility and to process SCRA reimbursement requests. RFS providea Ginnie Mae management, Account Executives and analysts with access to loan level data and pool level data, pool accounting data, external agency and related data for use in issuer and securities monitoring, policy enforcement, and analysis as needed. Issuers, trading partners, and other authorized parties also will have access, depending on security profiles, to RFS loan and pool level data as approved by Ginnie Mae. RFS also uses the collected PII data to verify against existing records.</p> |
| 8. | With whom is the PII data shared (other agencies, organizations, systems, etc.)? |
| | <p>RFS receives and provides MBS-related data to a number of providers of data (issuers, trading partners), users of data (Ginnie Mae staff and investors), and processors of data (contractors, contractor systems, as in GinnieNET and IPMS). Personally identifiable information collected by RFS will not be shared with external agencies or organizations.</p> |
| 9 | What specific legal authorities, arrangement, and/or agreement authorize the collection of information (i.e. must include authorities that cover all information collection activities, including Social Security Numbers)? |
| | <p>The MBSAA RFS program is granted authority by Ginnie Mae to collect the subject information in accordance with the Ginnie Mae charter and mission to manage the Mortgage-Backed Securities portfolio and conduct associated tasks.</p> |
| 10. | How is the PII data secured? |
| | <p>Adequate security controls are in place in order to protect sensitive personal information. All RFS data is being transmitted over an secure VPN connection. Only authorized personnel are allowed to access any PII at any time. Additionally, approved secure procedures have been implemented, including encryption mechanisms and additional standards to protect PII. At this time the following general standards apply:</p> <ul style="list-style-type: none"> • Internet based data exchange—HTTPS Verisign Certificates, 128 bit encrypted • FTP---Secure FTP via approved secure FTP products |

| | |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none"> • Direct Point To Point---Secure as approved for each issuer using such service <p>The criteria, procedures, controls and responsibilities regarding access to this type of data have been documented to comply with the intent of the Federal Information Security Management Act of 2002 for standards and guidelines on security and privacy. The HUD IT Security Manual indicates that the system manager is responsible for ensuring that access to information and data is restricted to authorized personnel on a "need-to-know" basis. Other than the minimum security controls mandated by NIST and HUD, following OMB 06-16 requirements are being observed for protection of PII:</p> <ul style="list-style-type: none"> • Time out functionality for remote access where user re-authentication is required after every 30 minutes inactivity. Note: As per HUD requirements this has been modified to timeout after 20 minutes of inactivity. • Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by the Deputy Secretary or an individual he/she may designate in writing. • Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. |
| 11. | <p>Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on form(s), and/or a system of records notice published in the Federal Register.) If notice was not published, why not?</p> |
| | <p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>Additional explanation if required:</p> |
| 12. | <p>Do individuals have an opportunity and/or right to decline to provide information?</p> |
| | <p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>Additional explanation if required:</p> |
| 13. | <p>Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?</p> |
| | <p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>Additional explanation if required:</p> <p>GNMA-RFS does not gain consent from individuals to use their personal information. Consent is not gained by GNMA-RFS because any PII contained within GNMA-RFS is the result of data being provided by the issuer community, or other external federal agencies.</p> |
| 14. | <p>Is this IT system a System of Record?</p> <p>A System of Record is any group of records collected from the primary source under the control of an agency from which information is retrieved by the name of an individual or by some identifying</p> |

| | |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | number, symbol, or other identifying particular assigned to the individual. For example, a system that collects credit scores of individuals and is searchable by name or SSN would be a System of Record. |
| | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Additional explanation if required: |
| 15. | Is this system part of another System of Record? If your system receives a feed containing PII data from another agency's system that collects the PII data from the public, then that other agency's system is the System of Record and they are the sponsor of the collection. For example, if your system uses data from FHA that the agency has collected directly from the public, then your system is not the System of Record (the FHA system is). |
| | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If yes, provide name of the System of Record and sponsor: |
| 16. | Has a Systems of Record Notice (SORN) been published/approved by OMB for the system? A SORN is a notice that is published in the Federal Register whenever a new System of Record is implemented or an existing System of Record has modifications that impact the privacy data it collects. |
| | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If yes, provide OMB form number and name: |
| 17. | Is the system currently being modified or will it be modified this year? |
| | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If yes, describe modification: |
| 18. | If the system is being modified, will the SORN require amendment or revision? |
| | A revised notice must be published in the Federal register if the planned modifications to the System of Record will impact the privacy data the system collects. |
| | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If yes, explain: |
| 19. | What are the Retention Use and Disposal Practices? Guidance for this section should obtain from HUD retention use and disposal policy. It should also be validated that these procedures are outlined in the contracted service agreement to ensure that the contracted system does not hold onto data after services are no longer provided. |

| | |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>HUD program managers are responsible for preserving valuable HUD documents and data. Some documents and data are of value only for the short-term, others more long-term, and selected documents and data are of historical value and therefore should be transferred to the National Archives and Records Administration (NARA) for public access:</p> <ol style="list-style-type: none"> 1. Move inactive records out of high cost space in offices to lower cost storage space in Federal Records Centers. 2. Ensure that records of permanent value are identified, earmarked, and properly kept for later transfer to the National Archives. 3. Destroy records of temporary value when their retention periods end. <p>The following is the Ginnie Mae Retention Use and Disposal Policy:</p> <ol style="list-style-type: none"> 1. Ginnie Mae follow HUD records management laws, regulation, and policies 2. Ginnie Mae ensure all third party business partner location and all entities acting on behalf of them are managing records in accordance with HUD applicable laws, regulation, and policies 3. Ginnie Mae include records management practices as part of any scheduled oversight protocols. 4. Ginnie Mae do not maintain records longer than permitted 5. Ginnie Mae destroy records after retention requirement are met. 6. Ginnie Mae dispose of sensitive PII appropriately -use cross-cut shredder or burn bags for hard copy records and completely erase (not just delete) electronic records. <p>For more information please refer to" third party letter.pdf"</p> |
| 20. | How long is information retained? |
| | The Length of MBSAA GNMA-RFS information retained varies. It depends on the criticality of the information, documentation, and the PII information that was collected. MBSAA maintains the Records Disposition Schedule for Government National Mortgage Association Records. |
| 21. | Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)? |
| | Yes. Ginnie Mae retention schedule been approved by records officer and the National Archives and Records Administration (NARA). For more information please refer to RECORDS DISPOSITION SCHEDULE - Sch 64 GNMA Records - 8Feb08.doc |
| 22. | Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated. Specify the risk associated with retention of this PII. Will it be retained only as necessary? Please include a statement regarding the inadvertent collection of PII, and how it is documented and destroyed. |
| | Ginnie Mae is required to follow HUD retention policy. The appropriate media protection reduces the risk of identity theft by providing a means to properly identify, mark, store, transmit or destroy media or documents containing PII. Privacy protection must be an essential part of an information system's life cycle and include the procedures addressing the storage, irretrievability, accessibility, retention, and disposal of Sensitive But Unclassified (SBU) information. Personally Identifiable Information (PII) when lost compromised or disclosed without authorization could substantially harm an individual. |

| | |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>HUD requires that the information be maintained in the system or records electronic or paper that have the appropriate administrative, technical, and physical safeguard to protect the information. This responsibility extends to all third party business partners, such as Public Housing Authorities, grantees, and contractors, who are required to maintain such system of records by HUD.</p> <p>Third party business partners should take the following steps to help ensure compliance with these requirements:</p> <ol style="list-style-type: none"> 1. Limit Collection of PII <ol style="list-style-type: none"> a. Do not collect or maintain sensitive PII without proper authorization. Collect only the PII that is needed for the purposes for which collected. 2. Manage Access to Sensitive PII <ol style="list-style-type: none"> a. Only share or discuss sensitive PII with those personnel who have a need to know for purposes of their work. Challenge anyone who asks for access to sensitive PII for which you are responsible. b. Do not distribute or release sensitive PII to other employees, contractors, or other third parties unless you are first convinced that the release is authorized and proper. c. When discussing PII on the telephone, confirm that you are speaking to the right person before discussing the information and inform him/her that the discussion will include sensitive PII. d. Never leave messages containing sensitive PII on voicemail. e. Avoid discussing sensitive PII if there are unauthorized personnel, contractors, or guests in the adjacent cubicles, rooms, or hallways who may overhear your conversation. f. Hold meetings in a secure space if sensitive PII will be discussed (i.e., no unauthorized access or eavesdropping) and ensure that the room is secured after the meeting. g. Treat notes and minutes from such meetings as confidential unless you can verify that they do not contain sensitive PII. h. Limit distribution of any meeting notes or minutes that might contain sensitive PII. i. Record the date, time, place, subject, chairperson, and attendees at any meeting involving sensitive PII. 3. Protect Hard Copy and Electronic Files Containing Sensitive PII <ol style="list-style-type: none"> a. Clearly label all files containing sensitive PII by placing appropriate physical labels on all documents, removable media such as thumb drives, information systems, and application. Examples of the appropriate labels might include "for Official Use Only" or "for (Name of Individual/Program Office) Use Only." b. Lock up all hard copy files containing sensitive PII. c. Protect all media (e.g., hard copies, thumb drives, CDs, etc.) that contain sensitive PII d. Do not leave work folders containing sensitive PII unattended. This information should be maintained either in secured file cabinets or in computers that have been secured e. Keep accurate records of where PII is stored, used, and maintained. f. Periodically audit all sensitive PII holdings to make sure that all such information can be readily located. g. Secure digital copies of files containing sensitive PII. Protections include encryption, implementing enhanced authentication mechanisms such as two factor authentication, and limiting the number of people allowed access to the files. h. Store sensitive PII only on workstation that can be secured such as workstations located in areas that have restricted physical access. |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| | |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>4. Protecting Electronic Transmission of Sensitive PII via Fax, email, etc.</p> <p>a. When faxing sensitive PII, use the date stamp function , confirm the fax number, verify that the intended recipient is available, and confirm that he/she has received the fax. Ensure that none of the transmission is stored in memory on the fax machine, that the fax is in a controlled area, and that all paper waste is disposed of properly (e.g., shredded). When possible, use a fax machine that uses a secure transmission line.</p> <p>b. Before faxing PII, coordinate with the recipient so that the PII will not be left unattended on the receiving end.</p> <p>c. When faxing sensitive PII confidential information, use only individually-controlled fax machines, not central receiving centers.</p> <p>d. Do not transmit sensitive PII via an unsecured information system (e.g., electronic mail, internet, or electronic bulletin board) without first encrypting the information.</p> <p>e. When sending sensitive PII via email, make sure both the message and any attachments are encrypted.</p> <p>f. Do not place PII on shared drives, multi-access calendars, the intranet, or the internet.</p> <p>5. Protecting Hard Copy Transmissions of files Containing Sensitive PII.</p> <p>a. Do not remove records about individuals with sensitive PII from facilities where HUD information is authorized to be stored and used unless approval is first obtained from a supervisor and sufficient justification, as well as evidence of information security, has been presented.</p> <p>b. Do not use interoffice translucent envelopes to mail sensitive PII. Use sealable opaque solid white or Kraft envelopes. Mark the envelope to the person's attention.</p> <p>c. When using the U.S. postal service to deliver information with sensitive PII, double-wrap the documents (e.g., use two envelopes – one inside the other) and mark only the inside envelope as confidential with the statement "To Be Opened By Addressee Only."</p> |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Based on the authority of contractor representative, all data captured in this document is current and accurate.

Signature

Date

Printed Name

Title

Reviewed by:

Chitranjan Khandpur

Ginnie Mae Chief Privacy Officer

Date

Reviewed by:

Deborah V. Holmes

Ginnie Mae Chief Information Officer

Date